US GOVERNMENT PUBLIC KEY INFRASTRUCTURE

CROSS-CERTIFICATION METHODOLOGY AND CRITERIA

Version 1.0: March 2003

TABLE OF CONTENTS

FOREWORD

Objective

This document outlines the procedures and criteria for cross-certification of a PKI with the US Government's Federal Bridge Certification Authority (FBCA). Vendors who desire to demonstrate technical interoperability with the FBCA will follow a different process.

Background

In December 2000, the Federal Chief Information Officer's Council approved the FBCA Certificate Policy. The policy defines the FBCA as an interoperability mechanism for ensuring trust across disparate domains. Successful cross certification with the FBCA asserts that the Applicant Public Key Infrastructure (PKI) operates in accordance with the standards, guidelines and practices of the Federal Public Key Infrastructure Policy Authority (FPKI Policy Authority) and of the Federal PKI Steering Committee (FPKISC).

The FPKI Policy Authority is comprised of representatives of each Federal entity operating at least one PKI that is cross-certified with the FBCA. Its membership also includes representatives from the stakeholder agencies: Department of the Treasury, Department of Commerce, Department of Defense, Department of Justice, General Services Administration, and the Office of Management and Budget. In addition, the Chair, Federal PKI Steering Committee (FPKISC) participates with the FPKI Policy Authority in an advisory capacity. The FPKI Policy Authority is responsible for the oversight and management of the relationship between the FBCA and the member PKI's. Note that the FPKI Policy Authority may carry out some of the functions referred to in this document through its Certificate Policy Working Group (CPWG).

The FPKI Policy Authority is also responsible for recommending, to the FPKI Policy Authority Chair, the approval or rejection of applications for cross-certification with the FBCA. It is the authority for establishing procedures and standards for the FBCA.

The FPKISC supports the efforts of the FPKI Policy Authority. The FPKISC is responsible for the technical functionality of the FBCA and provides oversight to the FBCA Operational Authority. The FBCA Operational Authority performs the technical interoperability functions of the cross certification process.

For cross-certifications internal to the US Federal Government community, the FBCA Certificate Policy requires entities to sign a cross certificate Memorandum of Agreement (MOA) formally describing the terms and conditions of the cross certification. Cross certifications with non-Federal entities require the implementation of formal cross certification formal agreements between the US Government and the external entity. The details of these agreements may vary based on the nature of the external entity and its relationship to the Federal Government.

The Federal Chief Information Officer's Council provides oversight and support to the FPKI Policy Authority, and to the FPKI Steering Committee in their respective roles for directing and managing the FBCA.

Intended Audience

This document, which is issued under the authority of the FPKI Policy Authority, is intended for the use of information technology officials, PKI managers, and personnel involved in cross certification activities within the government and between government and external Certification Authorities.

These cross-certification guidelines should be read in conjunction with the FBCA Certificate Policy and the Criteria for Cross Certification document, available at http://www.cio.gov/fpkipa.

Readers can find further detail on the US Government FBCA at http://www.cio.gov/fbca. Requests for information can also be directed to **fpki.webmaster@gsa.gov.**

Definitions: The following terms are used in this guideline:

Affiliate: Approved cross-certified Applicant PKI that has successfully completed all steps required to become cross-certified with the Federal Bridge Certification Authority and has exchanged standard compliant cross certificates.

Applicant: the entity requesting cross-certification with the US Federal Bridge Certification Authority.

Bridge:the collection of hardware, software, policies, procedures and agreements that allow subscribers of unique PKI domains to rely on digital certificates issued by other PKI domains. A Certification Authority that only issues cross certificates for interoperability with other PKI domains and is not a "Trust Anchor."

Certification Authority (CA): the server platforms, software, and workstations used for (the purpose of) issuing and administering certificates and keys.

Certificate Policy (CP): a named set of rules that describes terms under which digital certificates are issued to subscribers, managed and revoked, and the requirements under which the CA must operate in order to maintain the trustworthiness of its issued certificates. A Public Key Infrastructure may adopt more than one Certificate Policy.

Certificate Policy Working Group (CPWG) – a subcommittee of the FPKI Policy Authority that is responsible for reviewing the CPs of Applicant Public Key Infrastructures and for performing the policy mapping of the submitted policies to the FBCA policy on behalf of the FPKI Policy Authority and of advising the FPKI Policy Authority at which level of assurance the applicant CPs would map to the FBCA CP. The CPWG recommends changes in the FBCA CP to the FPKI Policy Authority for approval.

Certification Practices Statement (CPS): a document that sets out the practices that the CA operational entity employs to implement the requirements of the CP. It is a comprehensive description of such details as the precise implementation of service offerings and procedures of public key certificate life-cycle management. The Certification Practice Statement is more detailed than the Certificate Policies supported by the Public Key Infrastructure.

Cross-Certificate: a certificate used to establish a trust relationship between two Public Key Infrastructures.

Cross-Certification: the process undertaken by Public Key Infrastructures to establish a trust relationship. When two Public Key Infrastructures cross-certify, they agree to trust and rely on each other's public key certificates and keys as if they had issued them themselves.

Digital Signature: a digital file that is the result of a transformation of a message by means of a cryptographic system using keys so that a person who has the initial message can determine:

(a) Whether the transformation was created using the key that corresponds to the signer's key; and

(b) Whether the message has been altered since the transformation was made.

Employee: any person employed by an organization and being issued a certificate in that.

External subscriber: any person not an employee who is issued a certificate. This category includes a member of the public, a client of, or supplier to, the issuing entity and may include a service-provider such as a consultant under contract to the entity who is issued a certificate in the capacity of service-provider.

Federal Bridge Certification Authority (FBCA): the U.S. Government's mechanism for enabling trust domain interoperability.

Key: a sequence of symbols that controls digital signature and encryption processes.

Public Key Certificate: a digital file that contains the public key of a subscriber together with related information, digitally signed with the private key of the Certification Authority that issued it.

Public Key Infrastructure (PKI): the entire set of policies, processes, and Certification Authorities used for the purpose of administering certificates and keys. This also designates the person or organizational unit within a department responsible for:

(a) The operation of a Certification Authority trusted by one or more users to issue and manage public key certificates and certificate revocation mechanisms; or

(b) The management of:

(i) Any arrangement under which an entity contracts for the provision of services relating to the issuance and management of public key certificates and certificate revocation lists on its behalf; and

(ii) Policies and procedures within the entity for managing public key certificates issued on its behalf.

A PKI remains at all times responsible and accountable for managing the public key certificates it issues or arranges to be issued on behalf of its organization.

Repository: a system for storing and accessing certificates or other information relevant to certificates.

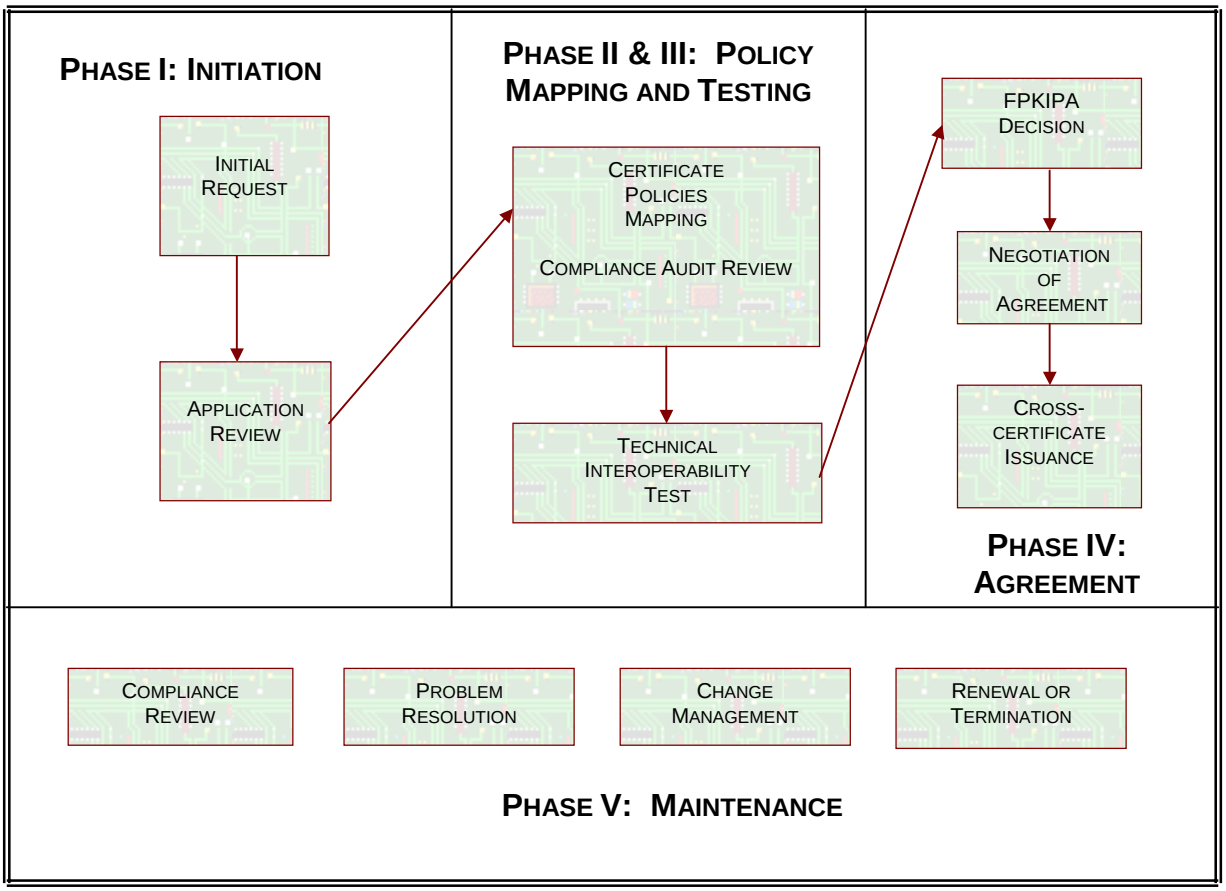
Standard: a level of attainment regarded as a measure of adequacy; requirements and guidelines approved for government-wide use.

Subscriber: a person whose public key is certified in a certificate. In the US Government, subscribers are employees and external subscribers.

PART ONE: METHODOLOGY

US Government FBCA – Cross-Certification Process

A request to cross certify with the US Government FBCA triggers a multi-phase process designed to achieve a mutually reliable trust relationship.



US Government Cross-Certification Process

Phase I – Initiation

- Request by Applicant PKI to cross-certify with the FBCA.
- Initial review of policy, technical and legal issues.
- Determine if application is complete and if all submissions comply with requirements.
- Determine if applicant is an appropriate applicant for cross certification.
- FPKI Policy Authority decision to reject request or proceed to next phase.

Step 1: Initial Request:

Purpose: To prepare and submit the required information to cross-certify with the FBCA.

Activities:

1. The Applicant PKI contacts the FPKI Policy Authority to initiate the process to allow it to cross-certify with the FBCA. A preliminary discussion is held to determine the applicant's suitability and readiness to pursue cross-certification.

2. The FPKI Policy Authority directs the Applicant to the website where documents and information can be found to assist in the cross certification process. These documents include:

   a. FBCA Certificate Policy Mapping Matrix
   b. Application for Cross Certification,
   c. X.509 Certificate Policy for the FBCA,
   d. This Criteria and Methodology document,
   e. Memorandum of Agreement template,
   f. Registration Form for Critical personnel (Non-Federal Applicants only),
   g. Applicant Technical and Personnel Authorization template

   If required, the FPKI Policy Authority will execute a non-disclosure agreement (NDA) to assure the applicant that all material presented during the application process will be treated in compliance with the terms of the agreement.

3. The Applicant PKI completes the application for cross certification. The Applicant PKI can seek assistance from the FPKI Policy Authority's in completing or revising the application. The Application includes the following information:

   a. Information on the Applicant's organization,
   b. Reason for requesting cross certification (non-Federal PKIs only);
   c. Information about the Applicant's Certificate Policy and Certification Practices Statement
   d. Information about the Applicant's PKI architecture
   e. Information about the Applicant's directory infrastructure
   f. Information about the Applicant's auditing practices
   g. Information about the Applicant's technical configuration (i.e. cryptographic algorithms, web portals, etc.)
   h. The proposed level of assurance at which cross-certification is sought.

4. If the Applicant PKI is an organization not governed by the Federal Information Processing Standards (FIPS) (i.e., a non-Federal Applicant PKI), it may be asked to provide additional information, such as but not limited to the following:

a. Evidence of the current legal status of the organization operating the PKI;
b. Evidence of the financial capacity of the organization operating the PKI (such as bonds, letters of credit, insurance demonstrating the organization's ability to meet the financial responsibilities associate with operating a PKI)
c. A signed agreement not to disclose any security-related information revealed for the purposes of facilitating cross-certification; and
d. Evidence of the financial capacity of the organization operating the PKI (such as bonds, letters of credit, insurance demonstrating the organization's ability to meet the financial responsibilities associate with operating a PKI)
e. The Applicant PKI submits the completed Application (which has been signed by the appropriate senior officials) to the Chair of the FPKI Policy Authority. One copy each of the Applicant's Certificate Policy, Certification Practices Statement and a completed Compliance Audit Report must accompany the form. The Applicant identifies a principal point of contact (POC). If the Applicant has conducted a CP mapping matrix, the FPKI Policy Authority would appreciate receiving an electronic copy of that document, as well, to facilitate formal policy mapping. The Applicant may seek the FPKI Policy Authority's advice on completing or revising the Application. Submission should be made in both writing (hardcopy/wet signature) and electronically (.doc, .rtf, .pdf, .wpd, etc.) to the Chair of the FPKI Policy Authority at the physical and electronic addresses shown on the FPKIPA website: http://www.cio.gov/fpkipa.

Step 2: Review and Decision Point

Purpose: To establish the Applicant's suitability for cross certification and to decide whether to continue with the process.

Activities

1. The Chair of the FPKI Policy Authority, upon receipt of the completed Application Form and all supporting documentation, will conduct an initial review of the Application using criteria specified in Part Two of this document.

2. If necessary, the Chair may seek additional information from the Applicant to assist the FPKI Policy Authority in its review of the Application.

3. Within 30 calendar days of receiving the Application and all supporting documentation, the FPKI Policy Authority renders its decision on whether to proceed with the policy mapping.

4. The Chair communicates the decision to the Applicant, ensuring that the point of contact understands that a decision to proceed with the policy mapping process in no way implies eventual cross-certification.

If the decision is not to proceed with the cross certification process, the Chair sends a letter to the Applicant POC enumerating the reasons why the application for cross certification has been rejected.

If the decision is to proceed with the cross-certification process, the FPKI Policy Authority notifies the FPKISC, the CPWG, and the FBCA Operational Authority of its decision to proceed and forwards the Applicants documents to the CPWG.

Phase II - Certificate Policy Mapping

- Mapping of Certificate Policies
- Evaluation of Applicant Compliance report

Step 3: Mapping of Certificate Policies

Purpose: To examine the Applicant's Certificate Policy (ies) and to establish their equivalency with the FBCA Certificate Policy.

Activities

Note: This is a participatory process. The Applicant PKI will be required to provide a knowledgeable and authorized representative to the CPWG for the Certificate Policy mapping process.

1. The CPWG maps the Applicant's Certificate Policy (ies) to the FBCA Certificate Policy, using the Certificate Policy Mapping matrix.
2. The CPWG reviews the Compliance Audit report and determines whether:
   a. The compliance auditor was a qualified independent third party
   b. The applicant's CPS is consistent with the applicant's CP, and
   c. The applicant is operating its PKI in compliance with its CPS.
3. The CPWG prepares a Certificate Policy Mapping Report, covering both the policy mapping and the compliant audit review, and forwards it to the FPKI Policy Authority Chair.
4. The Certificate Policy Mapping Report recommends one of the following:
   a. Proceed to the next step without conditions
   b. Proceed to the next step, with acceptance by Applicant of conditions; or
   c. Terminate process.
5. The FPKI Policy Authority reviews the CPWG Certificate Policy Mapping Report and decides whether to approve a mapping between the Applicants CP and the FBCA CP.
6. The FPKI Policy Authority Chair informs the Applicant of its decision.

If the decision is to proceed, then the process moves to Step 4 - Technical Interoperability Testing

Phase III - Technical Interoperability Test

Step 4: Technical Interoperability Testing

Purpose: The US Government has designated a FBCA Prototype CA, which is located at a facility contracted for the purpose to identify and resolve incompatibilities between the PKI technologies of the FBCA and applicant products and to minimize the risk of introducing incompatibilities with CAs already in the Production FBCA.

1. The FBCA Operational Authority reviews the cross certification application to prepare for the initial meeting with the Applicant.

2. The FBCA OA PM contacts the Applicant PKI POC to schedule an initial meeting to allow the FBCA OA and or Technical Lead to introduce and identify participants of the process and to discuss the technical interoperability testing process.

3. The FBCA OA teleconferences with key personnel to confirm architectural and key POC information. This provides information on the technical configuration of the Applicant to permit it and the FBCA Prototype Certification Authority to "inter-operate" at a technical level. (The Applicant's Certification Authority may be either its intended production or test-bed Certification Authority. If it is the Applicant's prototype Certification Authority, it must accurately represent the properties and specifications of the Applicant's production Public Key Infrastructure for the purposes of cross-certification.)

4. Having shared their respective technical data, the Applicant PKI and the FBCA OA undertake a test cross-certification with the Prototype FBCA. As this process is technology-dependent, it is not described here; however, it must demonstrate both:

    a. Successful exchange of PKI certificates,
    b. Directory interoperability, and
    c. The ability of each party to validate the other's CA certificates and cross certificates.

5. The FBCA OA documents the findings of the test in the Technical Analysis Report of the Agency Certification Authority Demonstration Report and forward a copy to the FBCA Technical Working Group (TWG) for review and recommendation. The Chair of the FBCA TWG prepares the Technical Analysis Report and provides a copy to the FPKI Policy Authority. The Report recommends one of the following:

    a. Proceed to the next step without conditions;
    b. Proceed to the next step, with acceptance of conditions; or

c. Terminate the process.

6. The FPKI Policy Authority reviews the Technical Analysis Report and decides whether to accept the recommendation.

7. The FPKI Policy Authority Chair informs the Applicant PKI's POC of the FPKI Policy Authority decision.

If the decision is not to proceed, then the Chair of the FPKI Policy Authority writes a letter to the Applicant detailing the reasons for the rejection.

If the decision is to proceed, then the process moves on to:

Phase IV – Agreement

- FPKI Policy Authority Decision
- Negotiation of Memorandum of Agreement
- Cross-Certificate Issuance

Step 5: FPKI Policy Authority Decision

Purpose: To decide whether to enter into a cross-certification agreement with the Applicant.

Activities

1. The Chair of the FPKI Policy Authority opens the floor to questions from the FPKI Policy Authority membership pertaining to the CPWG Mapping Report and Technical Analysis Report. Once all questions have been addressed, the Chair calls for a vote from the FPKI Policy Authority membership in accordance with the FPKI Policy Authority charter.

2. The FPKI Policy Authority decision contains one of three possible courses of action:

   a. Cross certify;
   b. Cross certify only with Applicant's acceptance of conditions; or
   c. Stay of proceedings while resolving outstanding issues;
   d. Reject the cross-certification request

3. Final approval for cross-certification requires a 75% majority vote by the membership.

4. By means of a decision letter, the Chair of the FPKI Policy Authority informs the Applicant's point of contact of the FPKI Policy Authority's decision.

5. If the FPKI Policy Authority fails to approve the application by a 75% vote, the Chair notifies the applicant via formal letter.

6. If the decision letter recommends conditional acceptance of the cross-certification request, the FPKI Policy Authority asks the Applicant to provide a written response within 30 calendar days of the date of the decision letter, or such other time as may be agreed.

    a. The CPWG or FBCA OA is responsible for repeating any step(s) in the process necessitated by a recommendation for conditional acceptance. The FPKI Policy Authority must be consulted again to approve resolution of major issues
    b. Following the resolution of all issues identified in the original letter of decision, the FPKI Policy Authority generates a second letter of decision for the signature of the FPKI Policy Authority Chair
    c. If the application receives approval, the Chair of the FPKI Policy Authority notifies the applicant by formal letter providing instructions for completing the Memorandum of Agreement.

Step 6: Negotiation of Memorandum of Agreement (MOA)

Purpose: To negotiate the terms and conditions of the cross-certification MOA.

Activities

1. In consultation with legal counsel, the FPKI Policy Authority determines which version of the template MOA is appropriate to use as a basis of discussion for drafting the final document.

2. Using the template MOA or another draft agreeable to both parties, the FPKI Policy Authority and the Applicant negotiate text for the proposed agreement. The FPKI Policy Authority provides any additional information or clarification required by the Applicant and vice versa. The parties reach final agreement on the content and language of the MOA and execute the document.

Step 7: Issuance of Cross-Certificates

Purpose: Allowing the FBCA OA and the Applicant PKI issue cross-certificates.

Activities

1. The Applicant submits a Technical and Personnel Authorization memorandum on official letterhead to the FPKI Policy Authority. The memorandum authorizes the FBCA to perform cross certification and is signed by the senior official responsible

for the operations of the Applicant CA. The memorandum includes the following information:

a. Key personnel, including primary and alternate technical and managerial contacts;
    i. Non-Federal Applicant critical personnel must also complete the registration form attesting to their identification and responsibility
b. Policy OID(s) for inclusion in the cross certificate;
c. Directory information tree for subject names in certificates issued by the Applicant;
d. Distinguished name of the CA;

2. Following the signing of the Memorandum of Agreement, the FPKI Policy Authority issues a letter of authorization to the Program Manager, FBCA OA, to initiate cross certification with the Applicant.

3. The FBCA OA reviews the Applicant Letter of Authorization (from 2 above).

4. The FPKISC, FBCA OA, and the Applicant contact determine an appropriate date for the cross-certification.

5. Following a satisfactory review of the technical data provided by both parties, the two Certification Authorities agree to issue cross-certificates and take the necessary procedural and technical steps to do so.

6. Appropriate notification concerning the cross-certification ceremony is provided to interested parties.

Phase V - Maintenance

Maintenance includes the following activities:

- Compliance Review
- Problem Resolution
- Change Management
- Renewal or Termination

It is important to ensure that, once in place and for its duration, the cross-certification arrangement continues to guarantee the agreed upon level of trust between the two parties. Each cross-certification is governed by the agreement entered into in Phase IV.

The maintenance phase provides mechanisms both for managing the relationship between cross-certified Certification Authorities as required for the proper operation of the arrangement, and for terminating the arrangement if either party contravenes its terms and conditions or at the desire of either party. The elements of this phase are not sequential and they will apply as circumstances warrant.

Compliance Review

Purpose - To determine if the Affiliated PKI is operating in compliance with its stated polices and practices.

Activities

The FPKI Policy Authority requests the Affiliated PKI perform a compliance audit. Although this audit may coincide with the review period specified in the Affiliate's CP, this is not required. In addition to annual compliance audit report submission by the Affiliated PKI to the FPKI Policy Authority, the FPKI Policy Authority may request that aperiodic audits be conducted and the compliance reports provided. All such requests shall be made for cause, and the cause shall be disclosed at the time of request.

Upon receipt, the FPKI Policy Authority provides the Compliance Audit Report to the CPWG for review.

1. The CPWG prepares a Compliance Review Report and provides a copy to the FPKI Policy Authority Chair. The Compliance Review Report will:
   a. Indicate no problem exists and recommend continuation of the affiliation unchanged.
   b. Indicate any deficiencies and suggest corrective action, but recommend that the Affiliated PKI continues to be cross certified at its current assurance level;
   c. Recommend renewal, but further recommend that the Policy Authority downgrade the assurance level of the cross certificate; or
   d. Recommend that the Policy Authority terminate the cross-certification

2. The FPKI Policy Authority Chair forwards the Compliance Review Report to the FPKI Policy Authority for action. If the problem cannot be resolved in a timely fashion, the FPKI Policy Authority may terminate the agreement, continue with conditions, or take other action as deemed necessary.

3. The FPKI Policy Authority Chair informs the FPKISC, FBCA OA, and Affiliated PKIs of the FPKI Policy Authority's decision.

Problem Resolution

Purpose: To report and correct problems the parties may encounter during the effective period of the cross-certification agreement.

Activities: Either party to the cross-certification arrangement may notify the other of problems and request resolution. Problem resolution procedures are specific to the problem encountered and will be agreed upon between the parties.

Change Management

Purpose: To manage changes to the FBCA or Affiliate PKI associated with a particular cross-certification agreement and to decide what actions to take as a result of implementing such changes.

Activities:

1. Either party to the cross-certification agreement may initiate this process. If either the FBCA or Affiliate PKI is contemplating changes that impact the terms of the agreement, then a notice of the change must be provided to the other party.

2. Each party reviews the notice and determines the appropriate response:

   a. Unconditional acceptance of the proposed change(s);
   b. Conditional acceptance, with follow-up required (the change is accepted but the next Compliance Review must pay particular attention to the change implementation); or
   c. The change is found to be unacceptable.

3. If a change implemented by one of the parties is deemed unacceptable to the other, such implementation may cause termination of the cross-certification agreement.

Renewal or Termination

Purpose: To decide whether to renew or terminate an existing cross-certification arrangement, and to specify the process for either renewal or termination.

Activities:

Should the FPKISC, the FBCA OA, or the FPKI Policy Authority become aware of any information that indicates that there has been a failure in the integrity of the Affiliated PKI that is deemed by any of the Entities to have the potential to adversely affect the security of the FBCA and its other affiliates, then the FPKI Policy Authority Chair, at his or her discretion, may instruct the FBCA OA to revoke the cross-certificate of the Affiliated PKI. The FPKI Policy Authority informs the Affiliate point-of-contact of the revocation. The FPKI Policy Authority Chair then informs the FPKI Policy Authority membership and other Affiliated Certification Authorities of the revocation.

A. Common Process

1. The FBCA OA provides the FPKI Policy Authority with a Renewal Notice indicating the cross-certificate is due to expire, so the FPKI Policy Authority may make a determination concerning renewal or termination. The notice will contain a summary of all relevant issues and information from various documents, including:

    a. The most recent Compliance Review Report;
    b. All Problem Resolution Reports since the arrangement was signed or last renewed; and
    c. All Change Management Reports since the arrangement was signed or last renewed.

B. Renewal of Existing Arrangement with an External PKI

1. The FBCA OA notifies the FPKI Policy Authority 180 days before the expiration date of any cross-certification agreement, to provide the FPKI Policy Authority time to consider whether to renew it.

2. The FPKI Policy Authority contacts the Affiliate to ascertain whether there is interest in renewing the agreement, and to seek any information the party may wish the FPKI Policy Authority to consider in its deliberations.

3. The FPKI Policy Authority reviews the Renewal Notice and decides either to:

    a. Recommend the FPKI Policy Authority Chair renew the agreement, for a specified period of time, with no changes; or
    b. Enter into negotiations to revise the cross-certification agreement and, depending on the outcome of the negotiations, subsequently to recommend to the FPKI Policy Authority Chair to enter into the agreement.
    c. Terminate the agreement.

4. If the FPKI Policy Authority decides that the agreement be renewed with no changes, it informs the Affiliate.

5. If the FPKI Policy Authority decides to negotiate a new agreement, it informs the Affiliate in writing. If the Affiliate wishes to proceed, then the usual procedures will apply.

6. If the FPKI Policy Authority decides to terminate the agreement or the Affiliate declines the FPKI Policy Authority recommendation, the agreement will expire according to its own terms.

C. Affiliate PKI Request for Termination of Agreement

1. Any party to an external cross certification agreement may submit a termination request at any time during the life of the agreement. The request must include the reason(s) for seeking termination, and the desired termination date.

2. The FPKI Policy Authority, in consultation with the FBCA OA and the Affiliated PKI's point of contact, determines a mutually agreeable termination date. The FBCA OA and the Affiliate PKI carry out the appropriate termination procedures.

3. The FBCA OA notifies the FPKI Policy Authority upon the completion of all termination procedures and the revocation of cross-certificates.

4. The FPKI Policy Authority informs all Affiliated PKI's of the withdrawal.

D. Affiliate PKI's Removal from the FBCA

1. Pursuant to the FBCA Memorandum of Agreement, the FPKI Policy Authority may remove an Affiliate PKI from the FBCA for cause. The FPKI Policy Authority notifies the member in writing of this action, noting the reason(s) for removal and the termination date, as stipulated in the Memorandum of Agreement.

2. The FPKI Policy Authority applies the criteria in Part IV in making the decision to remove a member from the FBCA.

PART TWO: CRITERIA FOR CROSS CERTIFICATION

This document is intended to describe the elements to be considered by decision-makers as they respond to a Request for Cross-Certification (Request). There are four major phases to this process:

1. Initiation Phase
2. Policy Mapping Phase
3. Test Phase
4. Agreement Phase

The fifth phase, Maintenance is not part of the criteria for cross-certification but will be mentioned briefly at the end of this document.

GENERAL PRINCIPLES

The full benefits of public key cryptography will be achieved through the widespread cross-certification of Public Key Infrastructures. However, given the need to carefully allocate resources within the government, some parameters must be established in order to prioritize cross-certification activities.

> Note: ***It must be emphasized that cross-certification with the US Government Federal Bridge Certification Authority (FBCA) is not a right, nor should any discussions be considered a commitment to issue cross-certificates.***

Certificates are issued and revoked at the sole discretion of the FPKI Policy Authority. When the FBCA issues a cross-certificate to a non-federal entity, it does so for the convenience of the federal government. Any review by the FBCA of a non-federal entity's certificate policy is for the use of the FBCA in determining whether or not interoperability is possible, and if possible, to what extent the non-federal entity's certificate policy maps to the FBCA policy. A non-federal entity must determine whether that entity's certificate policy meets its legal and policy requirements. Review of a non-federal entity's certificate policy by the FBCA is not a substitute for due care and mapping of certificate policies by the non-federal entity.

Subject to this document, the US Federal Government will consider requests for cross-certification from any organization or government operating a Certification Authority if such cross-certification is in support of US Government initiatives, specifically to facilitate electronic business applications and operating programs that require security.

US Government agency applicants must be certified and accredited in accordance with the requirements of OMB Circular A-130 Appendix III and other relevant IT security policies.

All applicants for cross-certification with the FBCA must obtain unique policy OIDs in the standard ISO object identifier registry from the appropriate commercial or national registration authority. US Government agencies may obtain policy OIDs from the NIST Computer Security Objects Registry.

Conditions

At any point in the Cross-Certification Process, the FPKI Policy Authority will make a determination with respect to proceeding to the next step – at any stage of the process – with or without conditions. Proceeding to the next step with conditions means that the FPKI Policy Authority is of the opinion that some aspect of the Applicant's operational environment – based on a review of the documentation presented or test-bed results – indicates some concern as to whether the Applicant Certification Authority operates in an appropriately secure manner for the assurance level required. The creation and acceptance of conditions means that such concerns can be allayed with changes in the operations of the Applicant PKI and that such changes have to be made before any positive decision by the FPKI Policy Authority concerning cross-certification will be made.

A decision not to proceed means that the FPKI Policy Authority is of the view that the Applicant's PKI does not demonstrate that it can operate in a manner commensurate with one of the FBCA assurance levels.

1. Initiation Phase

Upon receipt of a Request for Cross-Certification, the FPKI Policy Authority will make a preliminary determination as to whether the Request is complete and all required documentation, as set out in the instructions for the Request for Cross Certification, has been submitted. This determination will precede the FPKI Policy Authority's consideration of the Request.

For non-US Federal agency applicants, a statement explaining why the applicant is applying for cross-certification with the FBCA must accompany the Request. This may include a written statement, signed by a senior official from a Federal entity, endorsing the request and stating the reasons for doing so.

Requests will be signed by an appropriate senior official (an officer or executive) of the organization responsible for the PKI who is authorized to commit the organization to completing the cross-certification process. Such a commitment would include bearing any expenses incurred by the organization during the cross-certification process, and the authorization of any submission of information or statement required from the Applicant. Generally, a Request will be considered if it is from:

1. A US Federal government entity,

2. A commercial organization if that organization does or where there are firm projections from a US Federal government entity that it will be doing a sufficient amount of interactions with the government;

3. A non-commercial organization, if it will assist in the furtherance of the government's political, economic, social or cultural objectives;

4. A US state, local, or tribal government; and

5. A country or a sub-federal government of another country, where it would be in the interests of the US's international relations to cross-certify.

External applicants, unless otherwise exempted, must provide evidence of the current legal status of the entity responsible for the PKI. A certificate from the authorities of the jurisdiction in which the organization was created, indicating that the organization is in good standing under the laws of that jurisdiction, may be requested for this purpose.

Non-governmental applicants may be requested to provide evidence of financial capacity to manage risks associated with the operation of a PKI. Financial capacity can be demonstrated if the organization can provide a copy of a performance bond, a letter of credit from a financial institution, a letter indicating that insurance has been put in place, or a commitment letter from a bonding company, financial institution or insurance company.

The purpose of this requirement is to demonstrate the organization's ability to meet any financial responsibility associated with operating a Certification Authority, including any liability to subscribers or others relying on certificates issued and digital signatures verifiable by reference to public keys in such certificates. The nature and sufficiency of the required financial capacity will be determined at the discretion of the Policy Authority on a case-by-case basis.

Legal status and financial capacity constitute some of the evidentiary requirements needed to lay a foundation of trust between the US Government and applicants. Applicants exempted from these evidentiary requirements are:

a. A US Federal entity;

b. A state, local, or tribal government;

c. A foreign state or government; or

d. Any other entity exempted from this requirement by the FPKI Policy Authority.

A Request will not be considered complete until the FPKI Policy Authority is satisfied that all relevant documentation, as set out in the requirements, has been submitted.

Generally, a recommendation to proceed shall be made if the FPKI Policy Authority is of the view that all of the following exist, demonstrating the ability of the applicant to manage a PKI and that the Applicant has;

- Certificate Policy(ies) (or equivalent) in place,

- Certification Practices Statement in place, and
- Security Policy (or equivalent) in place with respect to the protection of the Certification Authority;
- Compliance audit of the Applicant's Principal Certification Authority has been done;
- Processes are in place to enforce the Applicant's Certificate Policy
- Sufficient information, as identified in the FBCA Agency Application Checklist, has been provided with respect to the technology used by the Applicant;
- The technology used by the Applicant is compatible with the technology employed by the FBCA (standards compliant);
- The Applicant is seeking an appropriate level of assurance;
- Adequate information has been provided with respect to the legal status of the organization responsible for the Applicant's PKI;
- Adequate information has been provided with respect to the financial capacity of the Applicant and the financial capacity appears adequate for the operations of the Applicant PKI;
- In the case of US Federal entities, the PKI in question has been certified and accredited as required by OMB Circular A-130 Appendix III;

The Applicant PKI must provide a representative to assist the FPKI Policy Authority in evaluating its application. The applicant application will be evaluated for security, privacy, and operational considerations.

The Applicant must identify which of its Certificate Policies are to be considered for cross-certification with the FBCA. It must be recognized that the Certificate Policy (ies) and Certification Practices Statement(s) may or may not be combined into one document (Certificate Policy (ies)/Certification Practices Statement). In any event, the Policy Authority will examine specific elements within the Certificate Policy (ies) and evaluate the Applicant PKI as providing a level of assurance equivalent to a specific level identified in the FBCA Certificate Policy.

Certificate Policy documents may support multiple levels of assurance. Additional evaluation may be required to map the Applicant PKI to the appropriate level in the FBCA Certificate Policy.

Adherence to the PKIX Framework

Applicant Certificate Policies must follow a current or recent version of the Internet Engineering Task Force (IETF) Request for Comment (RFC) 2527, Internet X.509 Public

Key Infrastructure Certificate Policy and Certification Practices Framework. Presenting Certificate Policies in this format expedites the comparison with the FBCA Certificate Policy. The FPKI Policy Authority will map the FBCA and Applicant Certificate Policies by category and element for consistency.

2. Policy Mapping Phase

Policy mapping is a process of comparing and contrasting the Applicant PKI Certificate Policy to the FBCA Certificate Policy and evaluating the extent to which the applicant PKI demonstrates policies, practices and procedures consistent with those of the FBCA. The categories to be used are found in the Mapping Matrix. Any review of the Applicant PKI's Certificate Policy involves looking at each section of the document to determine whether each section is comparable or equivalent to its counterpart in the FBCA Certificate Policy.

Bear in mind that:

a. There may be more than one section that applies for each element;
b. There may be differences in section headings;
c. Some Certificate Policies may have a different number of sub-fields for each element in the Certificate Policy;
d. The Certificate Policy may refer to other documents such as the Certification Practice Statement. In this situation, if there is insufficient information present in the section, it must be flagged for additional consideration and further examination of the referenced documents;
e. There may be differences in terminology and usage. For example, the term "trusted" may have specific implications to one organization that do not carry over when compared to another organization's Certificate Policy.

The results of the policy mapping exercise are recorded in the Mapping Matrix. All categories and elements that are not found in the Applicant PKI's Certificate Policy must be noted in the Mapping Matrix Brief Assessment. If there is a requirement for additional information to support or detail the comment, additional documentation may be used as long as the information is referenced correctly.

Policy mapping is a subjective exercise. Equal degrees of protection can be accomplished using different means. Policy mapping is an exercise to determine the "equivalency" between different means in order to establish that the policies provide a comparable degree of assurance (or to what degree they differ). Once this equivalency is established, the construction of cross-certificates, representing the trust placed by each PKI in the other, is performed. It is expected that the Applicant PKI would also engage in a comparable policy mapping exercise to assure itself of the degree of assurance represented by the FBCA Certificate Policy in question.

Evaluation of Applicant's Information Technology Security and Policy Compliance

Trustworthiness of an Applicant PKI must be evaluated for the purposes of cross-certification. This requires the Applicant PKI implement a certificate policy enforcement process. A key element of the enforcement process must include independent compliance audits as defined in the Applicant PKIs Certificate Policy. Applicant PKIs must present evidence that their policy enforcement process is performed as stated. For example, evidence may include additional audit reports for various components of the Applicant PKI, such as subordinate Certification Authorities and Registration Authorities.

As Public Key Infrastructure/Certification Authority audit standards evolve and become more accepted, then adherence to an international standard, with verification through an independent audit performed by qualified auditors, may become a pre-requisite for cross-certification with the FBCA. Given the absence of such standards at this time, audits will be accepted when performed by independent third parties, with demonstrated knowledge of PKI systems using accepted auditing methodologies.

Performance of a compliance audit on the Applicant PKIs Principal Certification Authority is a pre-requisite for cross-certification with the FBCA. The compliance audit must demonstrate that the Principal Certification Authority is operated in accordance with its Certificate Policy and Certification Practice Statement. The Applicant PKI must deliver a summary of the Principal Certification Authority's compliance audit report to the Policy Authority as part of its cross-certification application.

US Federal government entities may elect to use Inspector General or other internal independent auditing capabilities to satisfy this requirement.

3. Test Phase

Technical interoperability testing is used to ensure technical interoperability between the FBCA and the Applicant Principal (Root) Certification Authority. The objective is to determine whether there can be a successful exchange of cross-certificates and directory interoperability. The FBCA will not issue cross-certificates before successful completion of the interoperability tests. The FBCA Operational Authority operates the FBCA prototype system on behalf of the US Government. It is configured to be a duplicate of the Production FBCA. The Applicants' Certification Authority technical personnel will be required to work with the Operational Authority to complete the technical interoperability testing.

An Applicant PKI may use a test-bed facility, set and configured in a manner identical to its production Certification Authority (the Certification Authority to be permanently cross-certified with the FBCA), or may use its production Certification Authority for the technical interoperability testing. Any costs incurred by the Applicant Certification

Authority resulting from technical interoperability testing will be the responsibility of the Applicant.

In preparing a technical interoperability report, the FBCA Operational Authority describes the results of the tests and provides it to the FPKI Policy Authority.

At a minimum, the technical interoperability test will demonstrate:

a. Network connectivity is achieved using all required protocols;
b. The directories of the FBCA and the Applicant are interoperable;
c. The cross-certificate is correctly constructed by the FBCA, and exchanged and recognized by the Applicant Certification Authority;
d. The cross-certificate is correctly constructed by the Applicant Certification Authority, exchanged with the FBCA, and recognized by the FBCA;
e. A test transaction, using a test subscriber of the Applicant PKI, can be successfully validated; and,
f. The ability to share revocation information between the FBCA and the Applicant PKI.

The Report will also include a description of deficiencies identified during the test. Deficiencies may include technical interoperability deficiencies and potential performance issues that were not specifically identified by the test criteria. The report will also include the anticipated consequences of the deficiencies and a recommendation by the FBCA Operational Authority.

The successful completion of the technical interoperability test and completion of a FBCA Agency Application Checklist for the Applicant PKI (Production Platform) should complete the technical requirements for cross-certification.

4. Agreement Phase

Negotiation of Cross-Certification Agreement

The overall evaluation of the Applicant's PKI compliance involves an assessment of the information collected in the technical interoperability testing and the results of the policy mapping. If these results reveal the Applicant PKI meets the requirements of a FBCA assurance level, and the Applicant accepts these results, the FPKI Policy Authority may commence negotiations for the purpose of entering into a Cross-certification Memorandum of Agreement.

The relationship between the US Government and an organization operating a PKI will be governed by the Cross-certification Memorandum of Agreement to be signed by the FPKI Policy Authority Chair on the recommendation of the FPKI Policy Authority. Any FPKI Policy Authority recommendation to do so follows a sufficient examination of an Applicant application and the negotiation of a draft cross-certification Memorandum of

Agreement in a form suitable to the FPKI Policy Authority. The Applicant PKI cognizant authority must also sign the agreement.

An assessment to determine whether an agreement is in a suitable form cannot be undertaken in the abstract. A model Memorandum of Agreement, intended as a guide, is available at www.cio.gov/fpkipa. Deviations from this model, while not preferred, may be necessary to achieve agreement.

Relationship Maintenance, Continuation and Termination

Upon execution of a Cross-certification Memorandum of Agreement and the issuance of cross-certificates, the FBCA and Applicant (now Affiliated) PKI enter into a relationship subject to periodic review. The agreement will specify the period for review.

The FPKI Policy Authority may terminate the agreement and revoke the cross certificate when it determines the affiliation is no longer in the US Government's interests.